Technische Universität München
Zentrum Mathematik
PD Dr. Ch. Karpfinger

Repetitorium zur Algebra

Frühjahr 2011, Thema Nr. 3

Aufgabe 1 Zeigen Sie: Eine ungerade Primzahl p ist Teiler einer Zahl n^2+1 mit $n \in \mathbb{N}$ genau dann, wenn $p \equiv 1 \bmod 4$ gilt.

Lösung. Es gilt

$$\begin{aligned} p \mid n^2+1 \text{ für ein } n \in \mathbb{N} &\Leftrightarrow -1 \text{ ist quadratischer Rest} \quad \bmod p \\ &\Leftrightarrow \left(\frac{-1}{p}\right) = +1 \\ &\Leftrightarrow (-1)^{\frac{p-1}{2}} = 1 \\ &\Leftrightarrow \frac{p-1}{2} \text{ ist gerade} \\ &\Leftrightarrow p \equiv 1 \mod 4\,. \end{aligned}$$

Aufgabe 2 Zeigen Sie: Ist G eine endliche Gruppe, so existiert eine natürliche Zahl n derart, daß G isomorph ist zu einer Untergruppe der alternierenden Gruppe $\mathfrak{A}_n$.

Lösung. Nach dem Satz von Cayley existiert ein Gruppenhomomorphismus

$$\varphi : G \to \mathfrak{S}_m\,, \text{ wobei } m := |G|\,.$$

Betrachte nun die Abbildung

$$\psi : \left\{ \begin{array}{ccc} \mathfrak{S}_m & \to & \mathfrak{S}_m \times \mathfrak{S}_m \\ \pi & \mapsto & (\pi,\pi) \end{array} \right. .$$

Diese Abbildung φ ist ein injektiver Gruppenhomomorphismus. Also ist

$$\psi \circ \varphi : G \to \mathfrak{S}_m \times \mathfrak{S}_m$$

ein injektiver Gruppenhomomorphismus. Die Gruppe $\mathfrak{S}_m \times \mathfrak{S}_m$ kann man wiederum als Untergruppe von $\mathfrak{S}_{2m}$ auffassen. Dann sind alle (π,π) gerade Permutationen. Also ist $\psi \circ \varphi : G \to \mathfrak{A}_{2m}$ ein injektiver Gruppenhomomorphismus; es ist $n = 2m$.

Aufgabe 3 (a) Beweisen Sie, daß

$$f := X^3 + X^2 - 2X - 1$$

in $\mathbb{Q}[X]$ irreduzibel ist.
(b) Zeigen Sie, daß f eine reelle Nullstelle α im Intervall $]1,2[$ besitzt.
(c) Zeigen Sie, daß neben α auch $-\frac{1}{\alpha+1}$ Nullstelle von f ist.
(d) Folgern Sie, daß $\mathbb{Q}(\alpha)$ ein Zerfällungskörper von f ist.
(e) Wieviele Elemente enthält die Galoisgruppe von f über $\mathbb{Q}$?

Lösung. (a) Angenommen, f ist reduzibel in $\mathbb{Q}[X]$. Dann ist f auch in $\mathbb{Z}[X]$ reduzibel, d. h. von der Form

$$f = (X-\alpha)(X^2+\beta X+\gamma).$$

In $\mathbb{Z}_2[X]$ gilt somit

$$\overline{f} = (X-\overline{\alpha})(X^2+\overline{\beta}X+\overline{\gamma}).$$

Somit hat $\overline{f}$ eine Nullstelle in $\mathbb{Z}_2$. Das ist ein Widerspruch, da $\overline{f}(\overline{0}) \neq \overline{0} \neq \overline{f}(\overline{1})$.
(b) Wegen $f(1) = -1 < 0$ und $f(2) = 7 > 0$ folgt mit dem Zwischenwertsatz, daß f eine Nullstelle im offenen Intervall $]1,2[$ hat.
(c) Es gilt

$$f\left(-\frac{1}{\alpha+1}\right) = -\frac{1}{(\alpha+1)^3} f(\alpha) = 0.$$

(d) Wegen $\alpha > 0$ gilt $\beta := -\frac{1}{\alpha+1} < 0$, so daß $\alpha \neq \beta$ gilt. Weiter gilt $\alpha, \beta \in \mathbb{Q}(\alpha)$. Nach Vieta gilt, wenn γ die dritte Nullstelle von f ist,

$$\alpha\beta\gamma = 1.$$

Somit ist $\gamma = \frac{1}{\alpha\beta} \in \mathbb{Q}(\alpha)$. Somit ist $\mathbb{Q}(\alpha)$ der Zerfällungskörper von f.
(e) Da die Erweiterung $\mathbb{Q}(\alpha)/\mathbb{Q}$ algebraisch, separabel und normal ist, ist sie galoissch. Für die Galoisgruppe G von f über $\mathbb{Q}$ gilt $|G| = [\mathbb{Q}(\alpha):\mathbb{Q}] = \deg m_{\alpha,\mathbb{Q}}$ für das Minimalpolynom $m_{\alpha,\mathbb{Q}}$ von α über $\mathbb{Q}$. Da f irreduzibel und normiert ist, ist f das Minimalpolynom. Wegen $\deg f = 3$, erhalten wir also, daß G genau drei Elemente enthält, damit gilt $G \cong \mathbb{Z}/3\mathbb{Z}$.

Aufgabe 4 Es sei L/K eine algebraische Körpererweiterung und $\sigma : L \to L$ ein K-Endomorphismus von L, also $\sigma|_K = id_k$.
Beweisen Sie, daß σ ein K-Automorphismus von L ist.

Lösung. σ ist injektiv: Denn der Kern von σ ist ein Ideal im Körper L, also gleich $\{0\}$ oder L. Wegen $\sigma(1) = 1$ ist der Kern nicht gleich L.
σ ist surjektiv: Dazu sei $\alpha \in L$ gegeben. Wir zeigen, daß α als Bild unter σ auftritt. Es sei $g \in K[X]$ das Minimalpolynom von α. Mit N_g bezeichnen wir die Nullstellenmenge von g in L, insbesondere gilt $\alpha \in N_g \subseteq L$. Für jedes $\beta \in N_g$ ist

$$X-\beta \mid g \text{ in } L[X] \text{ wegen } \beta \in N_g \subseteq L.$$

Wendet man nun σ auf die Koeffizienten an, so erhält man wegen $g \in K[X]$

$$X-\sigma(\beta) \mid g \text{ in } L[X].$$

Also ist mit β auch $\sigma(\beta)$ aus N_g.
Da σ injektiv ist, ist $\sigma|_{N_g}$ eine injektive Selbstabbildung der endlichen Menge N_g, d. h. eine Permutation von N_g. Es folgt $\alpha \in \sigma(N_g) \subseteq \sigma(L)$, also ist σ auch surjektiv.